UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/774,102	01/31/2001	Jonathan S. Goldstone	Q60463	1078

7590 06/30/2005

SUGHRUE, MION, ZINN,
MACPEAK & SEAS, PLLC
2100 Pennsylvania Avenue, N.W.
WASHINGTON, DC 20037-3213

EXAMINER	
KADING, JOSHUA A	
ART UNIT	**PAPER NUMBER**
2661	

DATE MAILED: 06/30/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/774,102	GOLDSTONE, JONATHAN S.	
	Examiner	Art Unit	
	Joshua Kading	2661	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *18 April 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-27* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-27* is/are rejected.

7)☒ Claim(s) *1 and 10* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claim Objections

1. Claims 1 and 10 are objected to because of the following informalities:

Claim 1, line 3 and claim 10, line 3 state, "the Internet". There is no antecedent basis for "the Internet." Therefore, it is suggested that this be changed to --an Internet--.

Appropriate correction is required.

Claim Rejections - 35 USC § 102

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

3. Claims 1-3, 5-8, 10-13, 15-19, 21-23, and 25-27 are rejected under 35 U.S.C. 102(e) as being anticipated by U.S. Patent 6,735,702 B1, Yavatkar et al. (Yavatkar).

Regarding claims 1, 5, 10, 12, 15, 16, 17, 18, and 19, Yavatkar discloses "a network system that prevents bandwidth congestion on a network, said system comprising:

an origin client router connected to a plurality of clients through an Internet connection, said plurality of clients including an attacking client, and wherein each of said plurality of clients has a respective address associated with it (*col. 15, lines 4-11 where the fact that the "watchdog agent" is monitoring for attacks means that the attacks originate from some place and this place is connected to the network; it should further be noted that throughout Yavatkar, the network operates using IP/TCP*);

a destination site router connected to a destination server (*col. 15, lines 4-11 where the monitored nodes are the equivalent to destination servers*), said destination site router or firewall or client further comprising a bandwidth congestion detector operable to detect a bandwidth congestion condition (*col. 16, lines 22-25 where the "watchdog agent" is used to detect the attack*) and a communication device operable to communicate said bandwidth congestion condition and said addresses to said plurality of clients (*col. 18, lines 54-60*);

a router-router connection between said origin client router and said destination site router, wherein said router-router connection provides a discrete amount of access bandwidth by which said client router and said destination site router can pass data traffic back and forth to each other (*col. 15, lines 4-11 where the given nodes are all connected through the network; further it is inherent that there is a discrete amount of access bandwidth by which data can be transmitted, no link or network has unlimited bandwidth, therefore each link must have a given value for bandwidth*);

wherein said bandwidth congestion detector detects a bandwidth congestion condition originating at said attacking client and directed to said destination server and

automatically informs said origin client router of said attacking client's respective address (*col. 18, lines 54-60 where the attack is the result of the bandwidth congestion as stated in col. 15, lines 63-64*), and wherein further, said origin client router prevents said address of said attacking client from causing further bandwidth congestion (*col. 18, lines 54-60 whereby reforming the routing tables effectively prevents the address of attacking client from causing further congestion*)."

Regarding claim 2, Yavatkar discloses "a method as claimed in claim 1, wherein said connection point through which said origination client(s) is blocked from accessing the Internet, is a connection point which is physically closest to said origination client (*col. 17, lines 20-27 where the fact that the attack is traced to a final node (even if it is not the exact source of the attack) means that connection point is the closest possible point to the origination client as can be traced, and that is what is blocked*)."

Regarding claim 3, Yavatkar discloses "a method as claimed in claim 1, further comprising: communicating an IP address of said origination client(s) responsible for said overload condition to said connection point(s) (*col. 18, lines 54-60 whereby reforming routing tables to not include the source of the attack the IP address of the origination client must be known and the routing tables of other nodes (connection points) must also be updated for the restructuring to take effect*)."

Regarding claim 21, Yavatkar discloses "a method as claimed in claim 1, wherein one or more of said destination servers are protected by a respective firewall and wherein said detection of said overload condition is carried out by one of said respective firewalls (*col. 17, lines 20-27*)."

Regarding claims 22 and 26, Yavatkar discloses "wherein said detection of said overload condition is carried out by said target destination server (*col. 15, lines 4-6 where the device operating the "watchdog agent" can be the target destination*)."

Regarding claims 23 and 27, Yavatkar discloses "wherein said detection of said overload condition is carried out by a respective target router operable connected to said target destination server (*col. 15, lines 4-7 where the "watchdog agent" can operate from a remote node connected to the target destination*)."

Regarding claim 6, Yavatkar discloses "a method in accordance with claim 5, wherein said informing is performed automatically by said destination router (*col. 16, lines 22-25*)."

Regarding claim 7, Yavatkar discloses "a method in accordance with claim 5, wherein said informing is performed by human intervention (*col. 16, lines 22-25*)."

Regarding claim 8, Yavatkar discloses "a method in accordance with claim 5 further comprising: informing a plurality of remote routers connected to the Internet of said attacking address (*col. 18, lines 56-60*)."

Regarding claim 11, Yavatkar discloses "a network system according to claim 10, wherein said communication of said identity of said origination client occurs automatically upon detection of said denial of service or other Internet-based attack (*col. 16, lines 22-25*)."

Regarding claim 25, Yavatkar discloses "a network system in accordance with claim 10 wherein said attack detector is located within a firewall device located between said destination server and said origination client (*col. 17, lines 20-27*)."

Regarding claim 13, Yavatkar discloses "a system in accordance with claim 12, wherein said destination site router further informs a plurality of other intermediate routers within the Internet or shared WAN routers in addition to said origin client router (*col. 18, lines 54-60*)."

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> **(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the**

> invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claim 24 is rejected under 35 U.S.C. 103(a) as being unpatentable over Yavatkar et al.

Regarding claim 24, Yavatkar lacks, "said preventing is performed until a human administrator intervenes after determining whether said attacking site should be permitted to gain access to the Internet." Although Yavatkar does not explicitly disclose the human administrator permitting access to the Internet, Yavatkar does strongly suggest this is the case (*col. 6, lines 12-18 where the ability of a human operator to send commands to nodes, instructing the nodes how to behave strongly suggests a human operator has the capability to allow or prevent a given address from accessing a node*). It would have been obvious to one with ordinary skill in the art at the time of invention to include the human operator allowing or preventing access to a given node for the purpose of allowing legitimate users to access the network while stopping malicious users from accessing the network. The motivation for not allowing malicious attacks to propagate through the network is to prevent network congestion and thus allow legitimate users to properly access the network (*Yavatkar, col. 15, lines 63-64*).

6. Claims 4, 9, 14, and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Yavatkar et al. in view of U.S. Patent 6,738,814 B1, Cox et al. (Cox).

Regarding claims 4 and 9, Yavatkar lacks what Cox discloses, "determining whether said blocked origination client should be permitted to gain access to the

Internet (*col. 4, lines 62-67 where the incoming address could still come from a blocked client and as such the address will be checked against a database to check validity*); and permitting said blocked origination client access to the Internet if it is determined that said blocked origination client should be permitted access to the Internet (*col. 4, line 67-col. 5, lines 1-3 where if the address is not on the list, that is it does not already have a connection setup or is not an attack, the connection is allowed*)." It would have been obvious to one with ordinary skill in the art at the time of invention to include the allowing an address or client access to the network for the purpose of allowing a legitimate user access. The motivation for having to check for a valid address is to confirm that the client or user is no longer or not at all associated with an attack that will cause congestion.

Regarding claims 14 and 20, Yavatkar further discloses, "prevent said attacking client from gaining access to the Internet (*col. 17, lines 20-27*)..." However, Yavatkar lacks what Cox discloses, "determine whether said attacking client is attempting to initiate an Internet-based attack (*col. 4, lines 62-67 where the incoming address could still come from a blocked client and as such the address will be checked against a database to check validity*); permit said attacking client to gain access to the Internet if it is determined that said attacking client is not attempting to initiate an Internet-based attack (*col. 4, line 67-col. 5, lines 1-3 where if the address is not on the list, that is it does not already have a connection setup or is not an attack, the connection is allowed*)." It would have been obvious to one with ordinary skill in the art at the time of

invention to include the allowing an address or client access to the network for the purpose of allowing a legitimate user access. The motivation for having to check for a valid address is to confirm that the client or user is no longer or not at all associated with an attack that will cause congestion.

Response to Arguments

7. Applicant's arguments filed 18 April 2005 have been fully considered but they are not persuasive.

Applicant makes the following arguments:

1) Yavatkar does not disclose "blocking the origination client or clients" of the attack from the network because the node identified in Yavatkar as being blocked is not the originating source.

2) There is no suggestion of disclosure in Yavatkar or Cox of "identifying an attacking address and then blocking the identified attacking address from accessing the Internet."

3) Cox lacks the identification of the originating client and then preventing access to the Internet of the originating client.

The examiner respectfully disagrees.

The following are reasons why Yavatkar and Cox read on applicant's invention as claimed:

1) Applicant cites col. 17, lines 22-24 of Yavatkar as evidence that Yavatkar does not disclose blocking the origination of the attack to the network. Although Yavatkar states that the node blocked may not be the originating source, Yavatkar does disclose that to the network (i.e. the Internet) the node blocked **is** "the source of the attack." Applicant's claims do not specifically state that the originating source is the node that is blocked (see claim 1, lines 8-10, "blocking the origination client...from accessing the Internet **through its...respective connection point**.") Assuming that applicant's claims did state the originating client was blocked at the source, Yavatkar would still read on the claimed invention because Yavatkar assumes that the edge node to the network of Yavatkar **is** "the source of the attack." Further, it would be questionable as to how a network under attack would block the attacking source if it were part of a completely independent, separate network. The network under attack has no authority to block or change routing information in any other network but its own. It light of the above arguments, it is believed that Yavatkar fully reads on applicant's claimed invention.

2) Yavatkar, col. 18, lines 54-60 disclose changing routing table information so as to prevent a source of an attack from accessing the network. Since the routing tables contain address information the attacking source address must be known and by changing the tables the network has effectively prevented access from the attacking source.

3) Cox was used to teach the deficiencies of Yavatkar corresponding to claims 4, 9, 14, and 20. Nowhere in claims 4 and 9 is there a disclosure of preventing an originating client from accessing the Internet. And as noted in the rejections above for

claims 14 and 20, Yavatkar discloses preventing access to the Internet as seen in col. 18, lines 54-60. Therefore, Yavatkar in view of Cox fully accounts for all of applicant's claimed limitations.

Conclusion

8. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

9. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Joshua Kading whose telephone number is (571) 272-3070. The examiner can normally be reached on M-F: 8:30AM-5PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Chau Nguyen can be reached on (571) 272-3126. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Joshua Kading
Examiner
Art Unit 2661

June 22, 2005

CHAU NGUYEN
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2600